FIG. 1

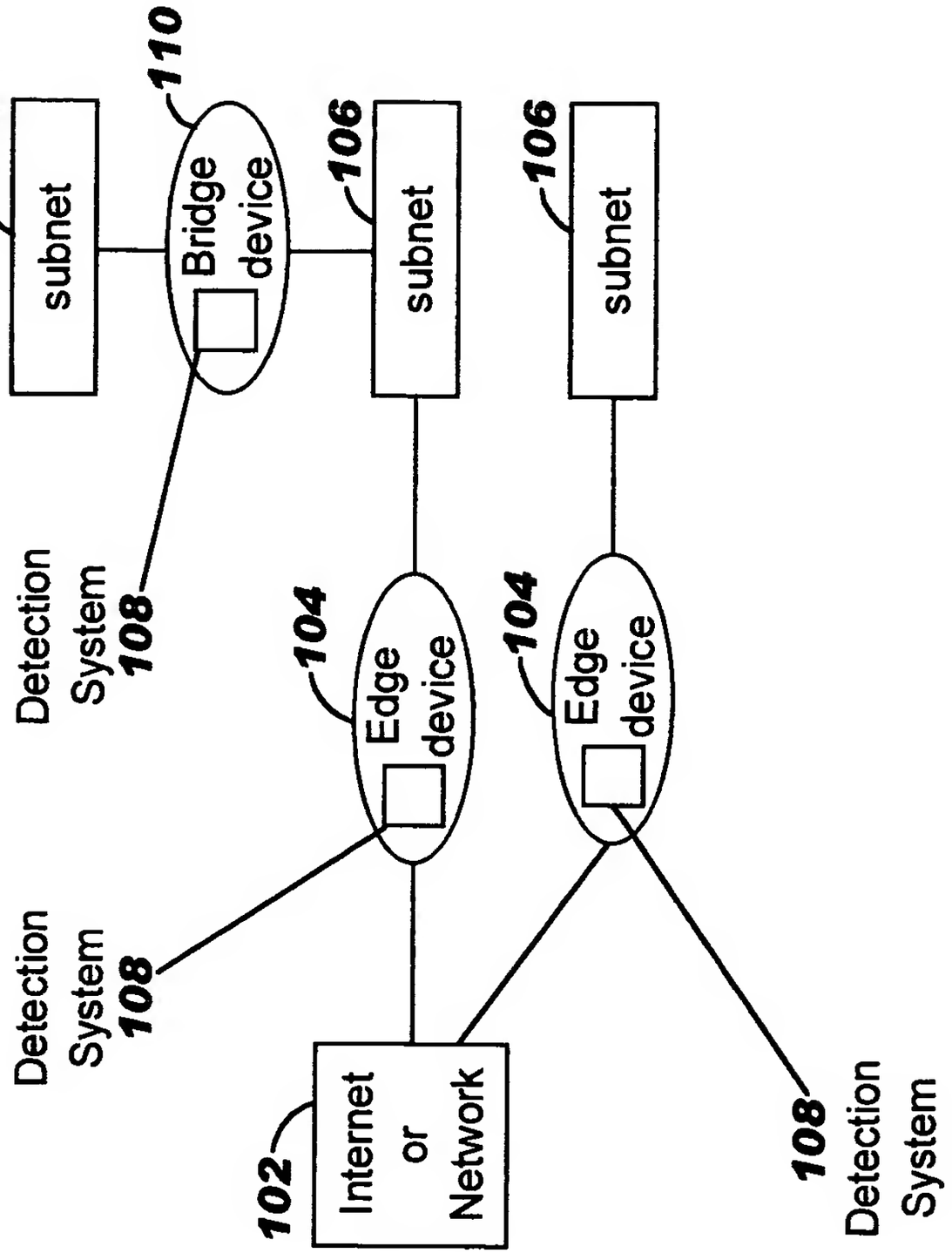

100
106
subnet
110
Bridge device
106
subnet
106
subnet
Detection System 108
104
Edge device
104
Edge device
Detection System 108
102
Internet or Network
108
Detection System

FIG. 2

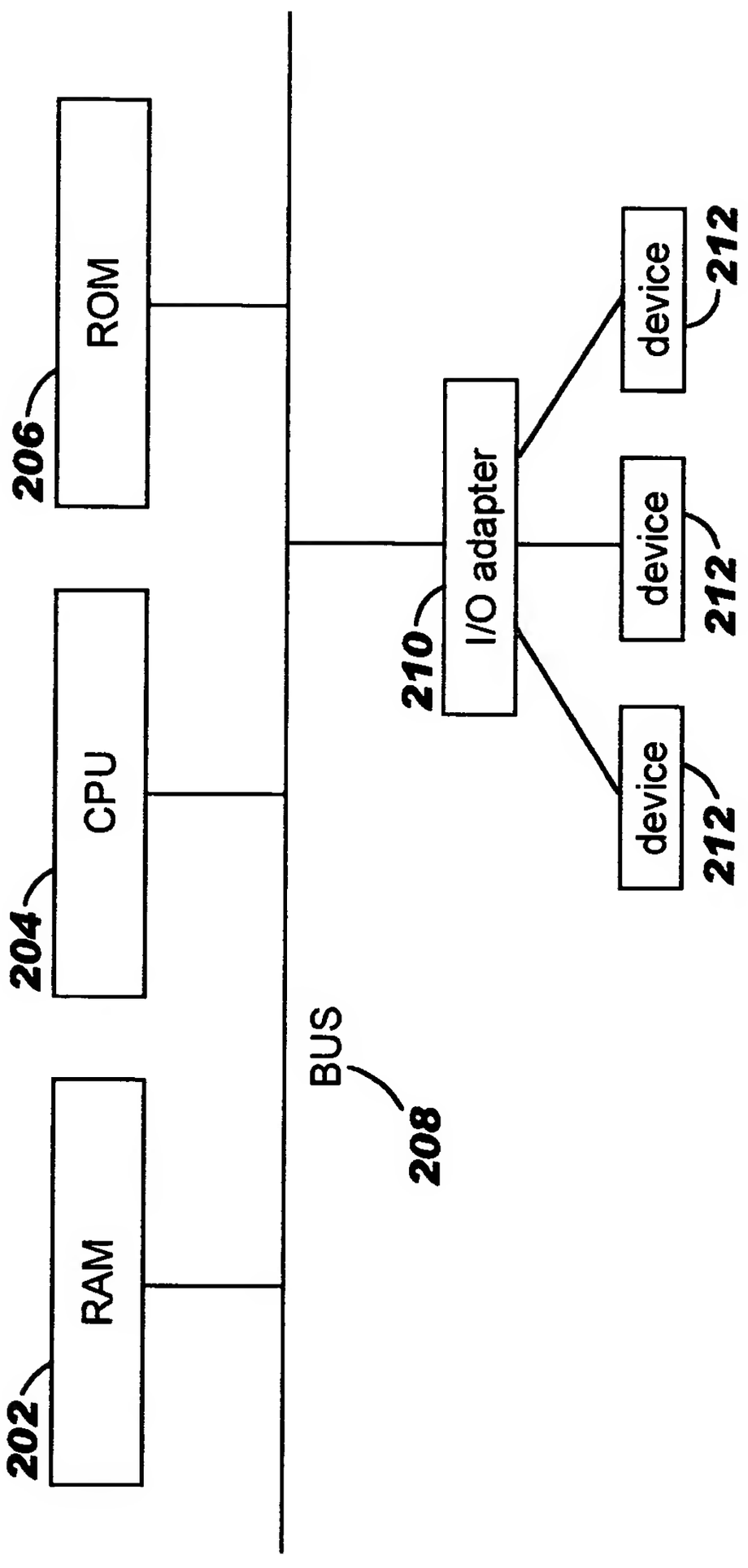

200
RAM
202
CPU
204
ROM
206
BUS
208
I/O adapter
210
device
212
device
212
device
212

FIG. 3

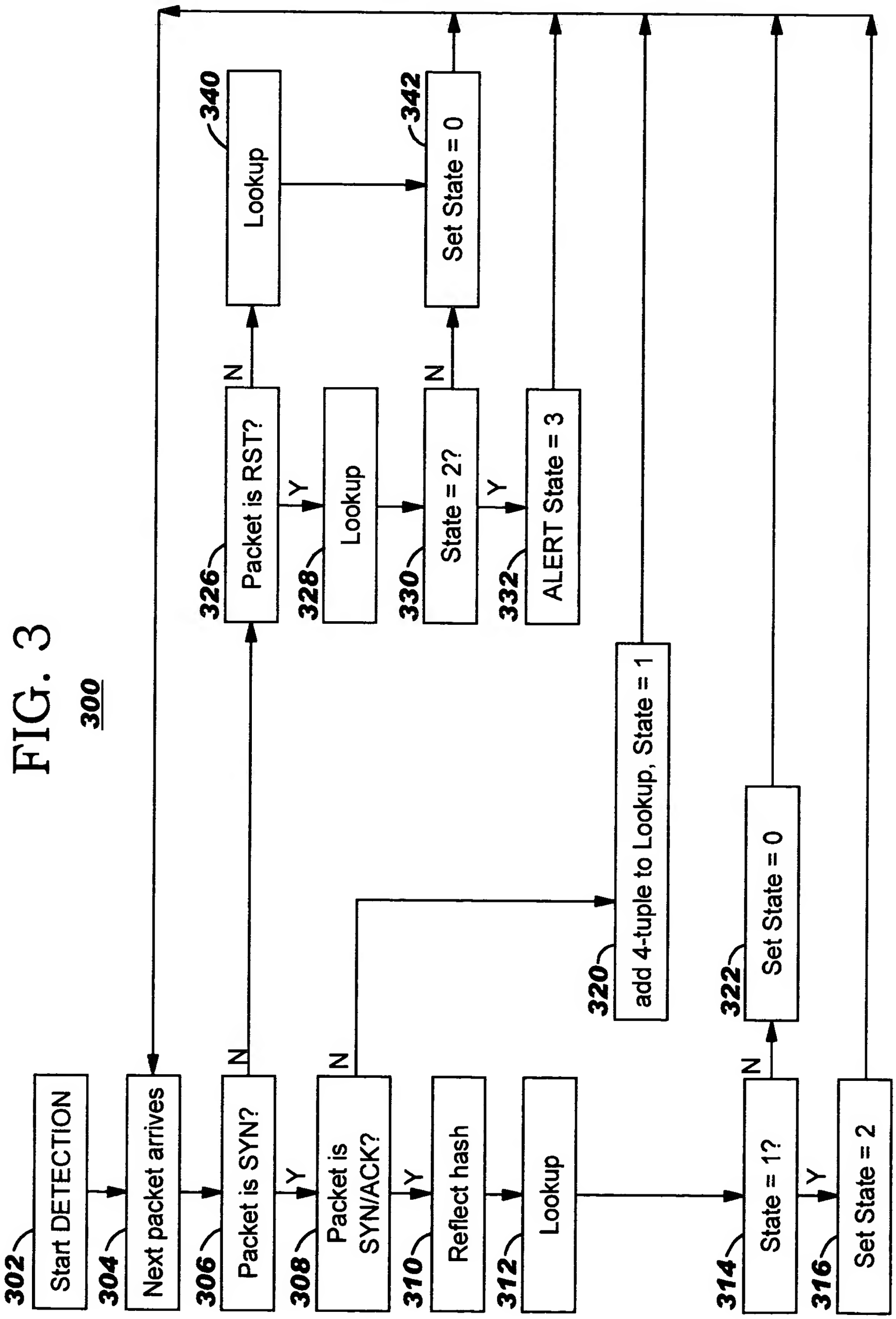

300
302 Start DETECTION
304 Next packet arrives
306 Packet is SYN?
N
Y
308 Packet is SYN/ACK?
N
Y
310 Reflect hash
312 Lookup
314 State = 1?
N
Y
316 Set State = 2
320 add 4-tuple to Lookup, State = 1
322 Set State = 0
326 Packet is RST?
N
Y
328 Lookup
330 State = 2?
N
Y
332 ALERT State = 3
340 Lookup
342 Set State = 0

FIG. 4

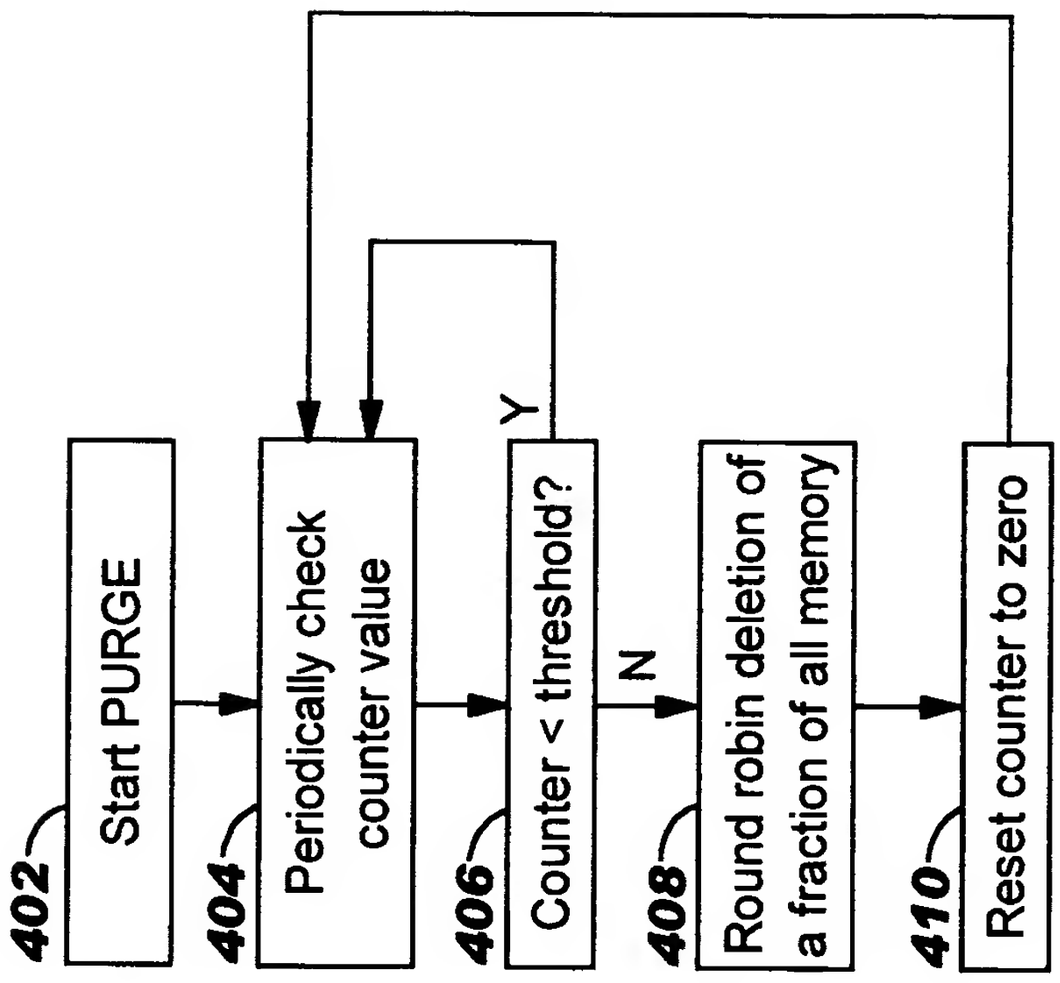

400
Start PURGE
402
Periodically check counter value
404
Counter < threshold?
406
Y
N
Round robin deletion of a fraction of all memory
408
Reset counter to zero
410

FIG. 5

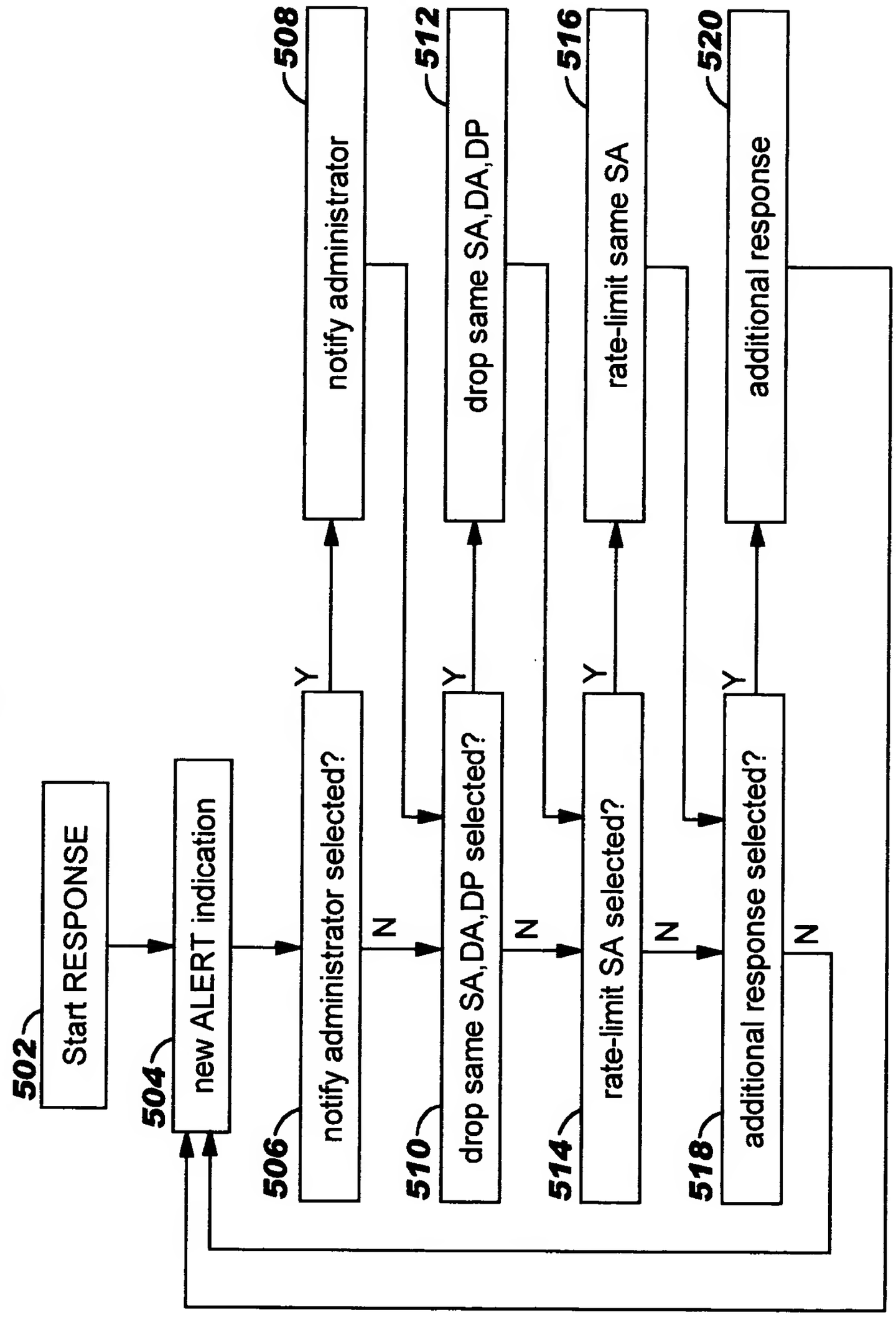

500
Start RESPONSE
502
new ALERT indication
504
notify administrator selected?
Y
notify administrator
N
506
drop same SA,DA,DP selected?
Y
drop same SA,DA,DP
N
510
rate-limit same SA selected?
Y
rate-limit same SA
N
514
additional response selected?
Y
additional response
N
518
508
512
516
520

FIG. 6

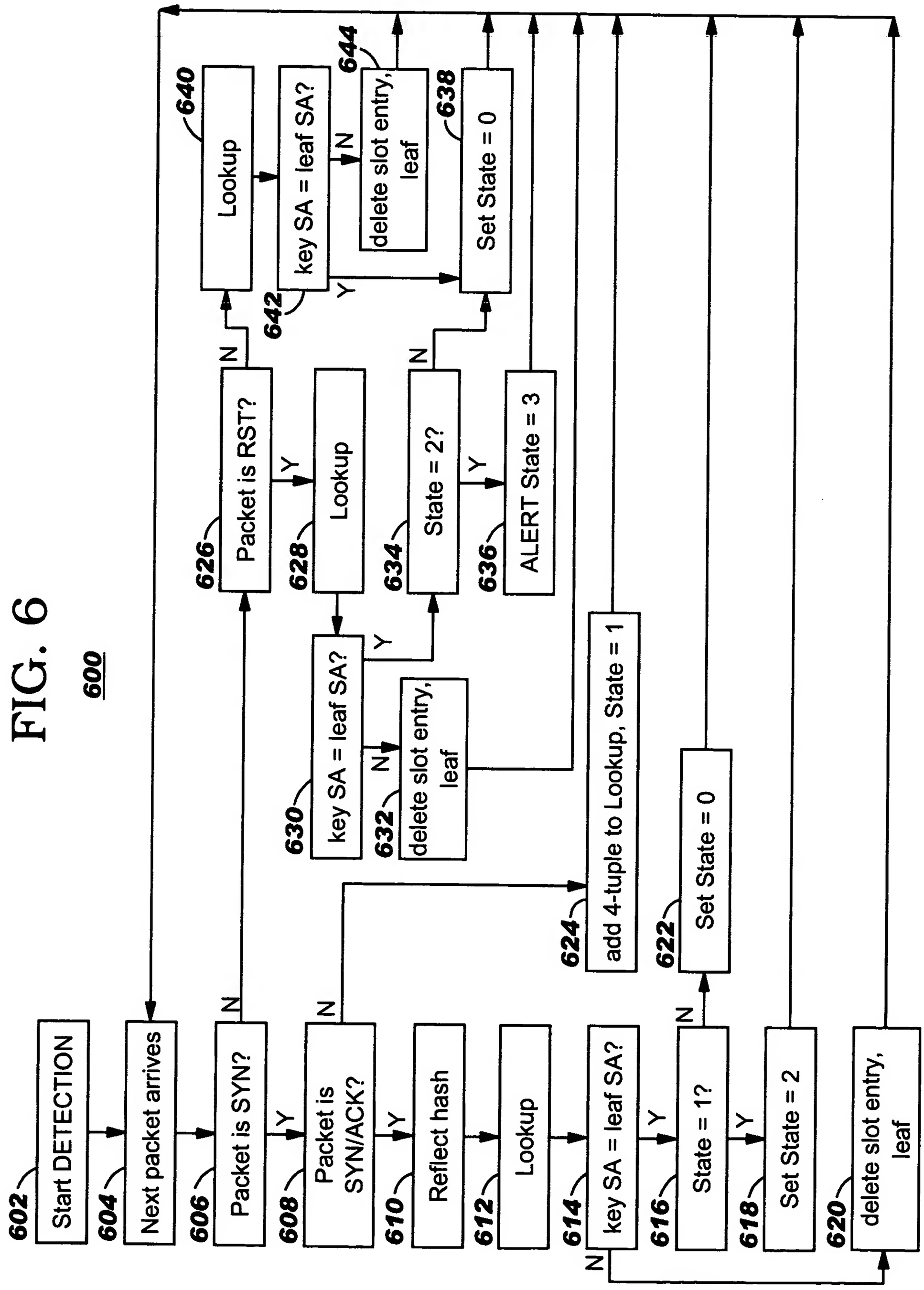

600
602 Start DETECTION
604 Next packet arrives
606 Packet is SYN?
608 Packet is SYN/ACK?
610 Reflect hash
612 Lookup
614 key SA = leaf SA?
616 State = 1?
618 Set State = 2
620 delete slot entry, leaf
622 Set State = 0
624 add 4-tuple to Lookup, State = 1
626 Packet is RST?
628 Lookup
630 key SA = leaf SA?
632 delete slot entry, leaf
634 State = 2?
636 ALERT State = 3
638 Set State = 0
640 Lookup
642 key SA = leaf SA?
644 delete slot entry, leaf
Y
N

FIG. 8

800

TCP Header Format

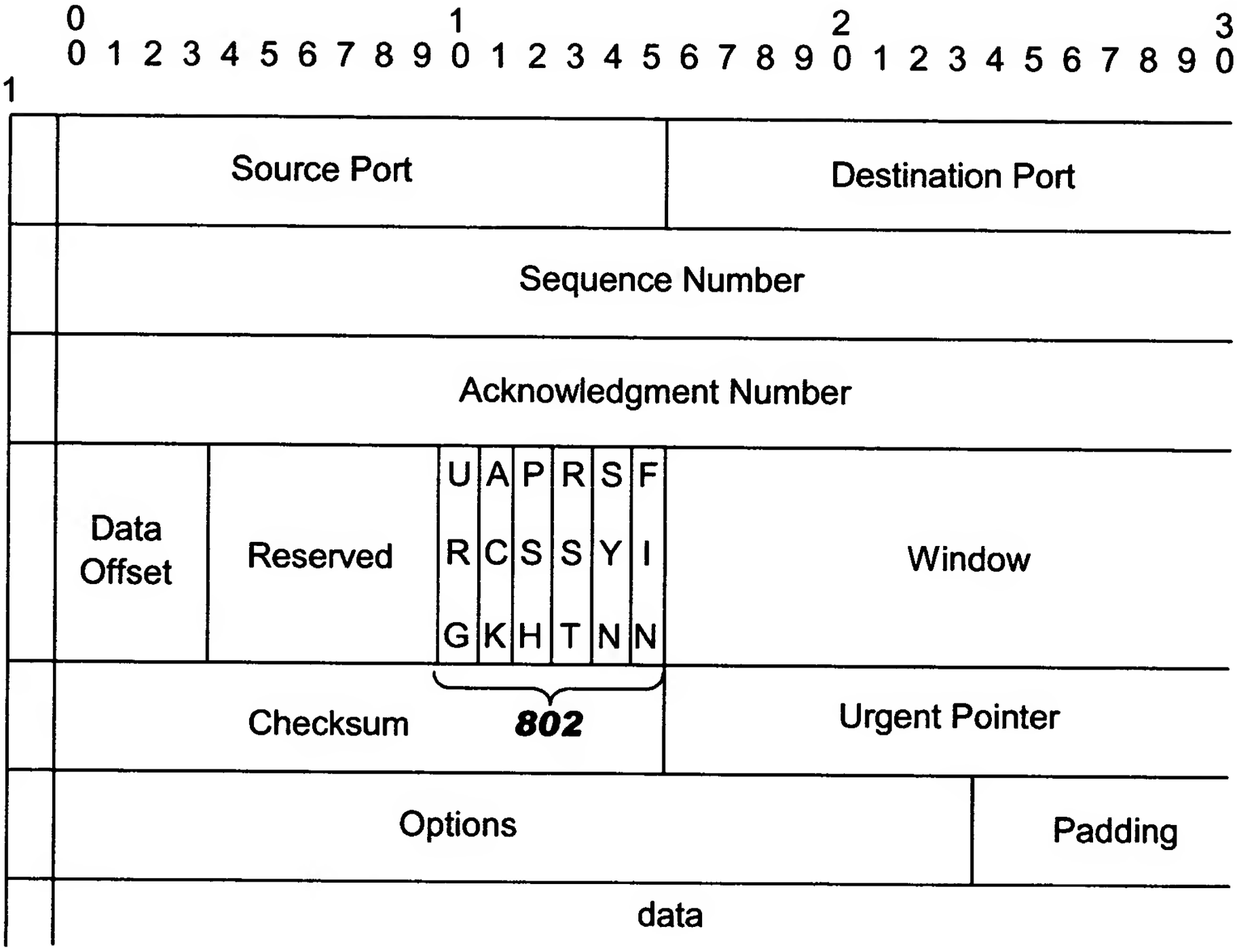


FIG. 7

700

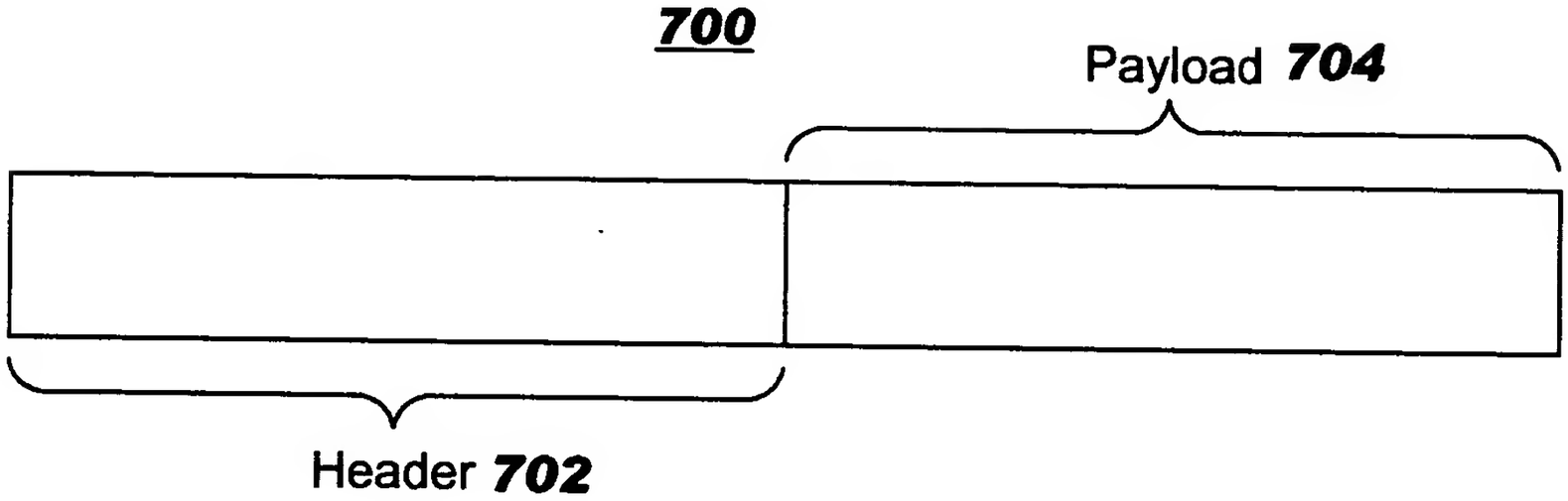


FIG. 9

900

0 4	8 16	19 31
Version / IHL	Type of Service	Total Length
Identification	Flags	Fragment Offset
Time To Live	Protocol	Header Checksum
Source IP Address		
Destination IP Address		
Options		Padding

FIG. 10

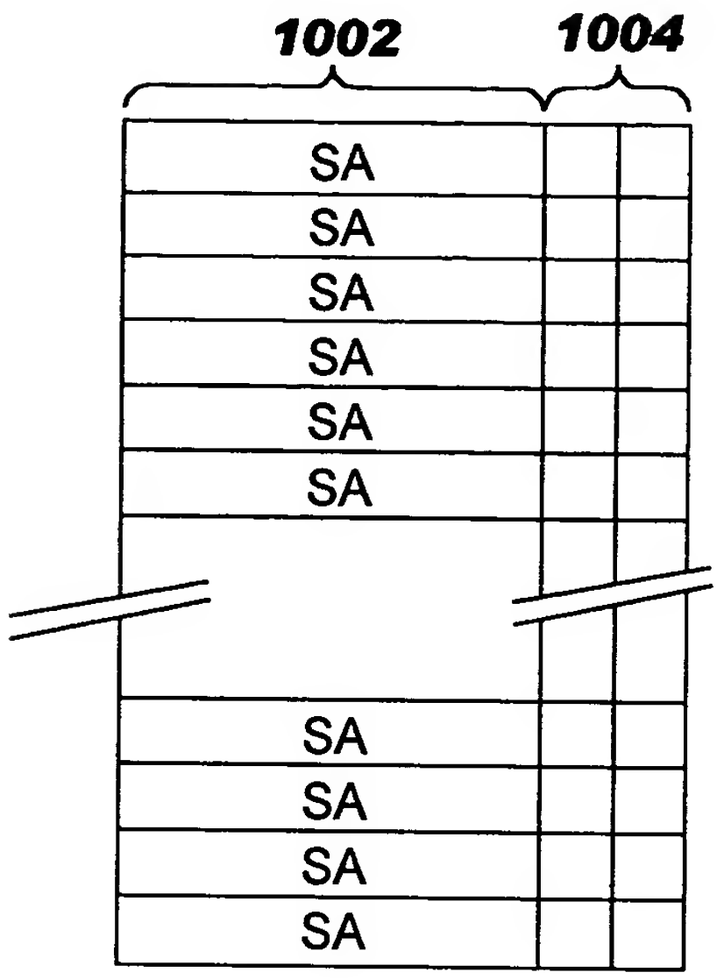
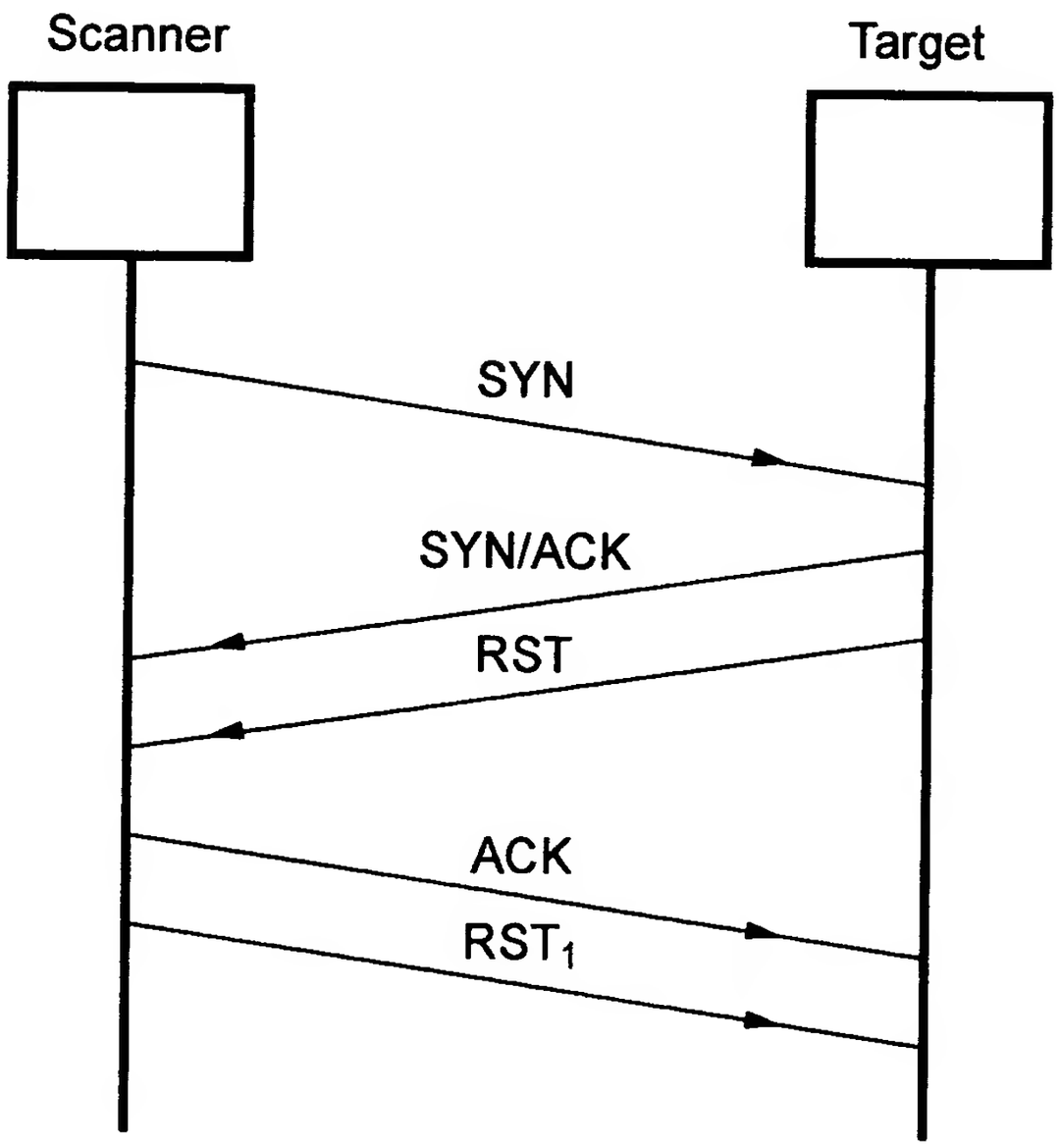

1000
1002
1004
SA
SA
SA
SA
SA
SA
SA
SA
SA
SA

FIG. 11


Scanner
Target
SYN
SYN/ACK
RST
ACK
RST1